(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
10. Juli 2003 (10.07.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/056428 A2

(51) Internationale Patentklassifikation[7]: G06F 11/00, G05B 19/042

(21) Internationales Aktenzeichen: PCT/DE02/04711

(22) Internationales Anmeldedatum:
23. Dezember 2002 (23.12.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 64 495.7 28. Dezember 2001 (28.12.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KRAM, Raimund** [DE/DE]; Fliederstr. 7a, 91056 Erlangen (DE). **BIRZER, Johannes** [DE/DE]; Friedhofweg 2, 92551 Stulln (DE). **HORN, Wolfgang** [DE/DE]; Maria-Reiff-Weg 5, 09337 Hohenstein-Ernstthal (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

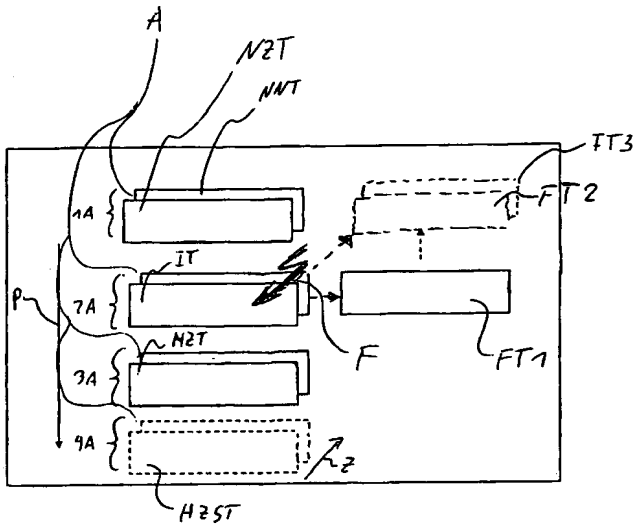
(81) Bestimmungsstaat *(national)*: US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

[Fortsetzung auf der nächsten Seite]

(54) **Title:** ERROR TOLERANT AUTOMATION SYSTEM OR METHOD FOR ERROR TREATMENT IN A REAL TIME AUTOMATION SYSTEM

(54) **Bezeichnung:** FEHLERTOLERANTES AUTOMATISIERUNGSSYSTEM BZW. VERFAHREN ZUR FEHLERBEHANDLUNG BEI EINEM ECHTZEIT-AUTOMATISIERUNGSSYSTEM



(57) **Abstract:** The invention relates to an automation system, wherein error (F) reaction is improved. This is achieved by means of a method for the treatment of errors in a real time automation system wherein at least one error reaction function (FT1, FT2, FT3) is triggered by at least one processing error (F) and/or access error (F). Said improvement is achieved by means of a method for the treatment of errors wherein the error reaction function (FT1, FT2, FT3) and by means of a method for the treatment of errors in an automation system which has at least two levels of execution (A), wherein at least one error reaction function (FT1, FT2, FT3) is triggered by at least one processing error (F) and/or one access error (F) on at least one of the other levels of execution (A).

[Fortsetzung auf der nächsten Seite]

WO 03/056428 A2

Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR)*

— *Erfindererklärung (Regel 4.17 Ziffer iv) nur für US*

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Automatisierungssystem, bei welchem die Reaktion auf Fehler (F) verbessert ist. Dies gelingt zum einen mit einem Verfahren zur Fehlerbehandlung bei einem Echtzeit-Automatisierungssystem bei dem durch zumindest einen Verarbeitungsfehler (F) und/oder Zugriffsfehler (F) zumindest eine Fehlerreaktionsfunktionsfunktion (FT1, FT2, FT3) ausgelöst wird, wobei die Fehlerreaktionsfunktion (FT1, FT2, FT3) parametrierbar und/oder programmierbar ist. Zum anderen gelingt eine Verbesserung durch ein Verfahren zur Fehlerbehandlung bei einem Automatisierungssystem, welches zumindest zwei Ablaufebenen (A) aufweist, bei dem durch zumindest einen Verarbeitungsfehler (F) und/oder Zugriffsfehler (F) in einer Ablaufebene (A) zumindest eine Fehlerreaktionsfunktion (FT1, FT2, FT3) in zumindest einer der weiteren Ablaufebenen (A) ausgelöst wird.

Beschreibung

Fehlertolerantes Automatisierungssystem bzw. Verfahren zur Fehlerbehandlung bei einem Echtzeit-Automatisierungssystem

Die Erfindung liegt auf dem Gebiet von Automatisierungssteuerungen bzw. Automatisierungssystemen. Automatisierungssysteme, bzw. -steuerungen werden insbesondere bei Produktionsmaschinen, Werkzeugmaschinen, Handhabungsautomaten, industriellen Prozessen und/oder in industriellen Fertigungen eingesetzt.

Automatisierungssysteme unterliegen verschiedensten Anforderungen, wie z.B. denen nach flexibler und/oder sicherer und/oder konsistenter Reaktion auf Ereignisse wie z.B.:

- Verarbeitungsfehler in einem Anwenderprogramm wie z.B. einer Division durch Null und/oder dem Verletzen von Arraygrenzen
- Zugriffsfehler bei I/O Variablen - Input/Output Variablen
- Zugriffsfehler beim Lesen und/oder Schreiben von Systemvariablen

Diese Anforderungen gelten insbesondere für ein frei programmierbares Automatisierungssystem bzw. -steuerung. Weist die Automatisierungssteuerung bzw. das Automatisierungssystem, wobei diese beiden Begriffe als Synonym füreinander stehen können, das Automatisierungssystem allerdings auch eine Automatisierungssteuerung mit aufweisen kann, Multitasking-Eigenschaften auf so verschärfen sich die Anforderungen. Dies gilt beispielsweise für ein frei programmierbares Automatisierungssystem für eine Produktionsmaschine, wie z.B. eine Druckmaschine, eine Kunststoffspritzgießmaschine mit Multitasking-Eigenschaften, die aufgrund integrierter Technologie- und Regelungsfunktionalität harten Echtzeiteigenschaften zu genügen hat. Echtzeiteigenschaften sind beispielsweise auch

bei einer Werkzeugmaschine, wie z.B. einer Drehmaschine, einer Schleifmaschine, einer Fräsmaschine, etc. oder auch bei einem oder mehreren in einem Verbund arbeitenden Handhabungsautomaten erforderlich.

Die Automatisierungssteuerung bzw. das Automatisierungssystem weist Software auf, wobei in dieser Software Tasks, d.h. Aufgaben bzw. Programme, bzw. Jobs gestartet und abgearbeitet werden, bzw. abarbeitbar sind. In einer Automatisierungssteuerung bzw. in einem Automatisierungssystem sind die obig beschriebenen Anforderungen insbesondere dann, wenn annähernd Echtzeitanforderungen zu erfüllen sind, bisher über synchrone Exceptions gelöst. Bei der synchronen Exception wird zumindest ein Anwenderprogramm, als Fehlerreaktion, unmittelbar mit der gleichen Priorität gestartet wie der bearbeitete Task, in dem ein Fehler aufgetreten ist.

Nachteilig bei dieser Lösung ist, dass die Lösung mit synchronen Exceptions in einem Automatisierungssystem bzw. in einer Automatisierungssteuerung mit hochprioren zyklischen Tasks nur bedingt einsetzbar ist, da die Gesamtlaufzeit der hochprioren zyklischen Taskebenen begrenzt ist. Beim Überschreiten dieser Begrenzung geht die Echtzeiteigenschaft verloren. Bei der Verwendung von synchronen Exceptions ist ein Echtzeit-Automatisierungssystem nicht realisierbar, da die Echtzeit nicht in jedem Fall garantiert ist. Allgemein tritt diese Problematik auch bei anderen Echtzeitsystemen auf, bei welchen hochpriore Tasks in einer maximalen Gesamtlaufzeit, welche für die Abarbeitung notwendig ist, abzuarbeiten sind.

Der Erfindung liegt die Aufgabe zugrunde, die Reaktion auf Fehler, welche in der Software (z.B. Division durch Null oder Verletzung von Arraygrenzen) und/oder Hardware (z.B. Zugriffsfehler bei I/O-Variablen) einer Automatisierungssteuerung bzw. einem Automatisierungssystem auftreten zu verbessern. Automatisierungssysteme, bzw. -steuerungen werden insbesondere bei Produktionsmaschinen, Werkzeugmaschinen, Hand-

habungsautomaten, industriellen Prozessen und/oder in industriellen Fertigungen eingesetzt.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren zur Fehlerbehandlung bei einem Automatisierungssystem, welches z.B. eine Automatisierungssteuerung ist, gelöst, bei dem bei zumindest einem Verarbeitungsfehler und/oder zumindest einem Zugriffsfehler zumindest eine Fehlerreaktionsfunktionsfunktion ausgelöst wird, wobei die Fehlerreaktionsfunktion zumindest parametrierbar und/oder programmierbar ist.

Die Parametrier- und/oder Programmierbarkeit einer Fehlerreaktionsfunktion ermöglicht es die Fehlerreaktionsfunktion derart auszubilden, dass die Echtzeiteigenschaften eines Automatisierungssystems auch im Fehlerfall erhalten bleibt. Von Automatisierungssystemen, insbesondere Echtzeit- Automatisierungssystemen, sind verschiedenste Forderungen zu erfüllen. Dies sind beispielsweise flexible, sichere und/oder konsistente Reaktionen auf:

- Verarbeitungsfehler im Anwenderprogramm, z.B. Division durch Null, Verletzen von Array-Grenzen,
- Zugriffsfehler bei I/O-Variable - Input/Output Variable,
- Zugriffsfehler beim Lesen und Schreiben von Systemvariablen.

Diese Forderungen sind beispielsweise insbesondere bei einem frei programmierbaren Automatisierungssystem für eine Produktionsmaschine mit Multitasking-Eigenschaften zu erfüllen, da diese z.B. aufgrund integrierter Technologie- und Regelungsfunktionalität harten Echtzeiteigenschaften zu genügen hat. Eine harte Echtzeiteigenschaft bedeutet, dass auch in einem Fehlerfall die Echtzeiteigenschaft bestehen bleibt. Bei Automatisierungssystemen ohne harte Echtzeit, d.h. z.B. im Fehlerfall ist die Echtzeiteigenschaft nicht mehr vorhanden, wurde die Behandlung eines aufgetretenen Fehlers bisher über synchrone Exceptions, welches Anwenderprogramme sind die un-

mittelbar mit der gleichen Priorität gestartet werden wie die bearbeitete Task/Aufgabe in der ein Fehler auftritt, gelöst.

Weist das Automatisierungssystem, d.h. die Automatisierungssteuerung verschiedene Ablaufebenen auf, so haben diese beispielsweise unterschiedliche Prioritäten. Programme, bzw. Funktionen, bzw. Tasks, bzw. Jobs (die engl. Begriffe sind teilweise auch synonym zu den deutschen verwendbar) sind in verschiedenen Ablaufebenen abarbeitbar. Tritt in einem Programm, bzw. einem Job, bzw. einer Funktion oder ähnlichem in einer Ablaufebene ein Fehler auf, so ist eine Fehlerreaktionsfunktions ausführbar, welche jedoch Programme bzw. Funktionen in den Ablaufebenen in ihrer zeitlichen Abarbeitung derartig beeinflussen kann, dass eine erforderliche Bearbeitungszeit eines anderen Programmes bzw. einer Funktion nicht mehr gewährt sein kann.

Eine Verbesserte Fehlerreaktion ist erfindungsgemäß auch dadurch erzielbar, dass zur Fehlerbehandlung bei einem Automatisierungssystem, welches zumindest zwei Ablaufebenen aufweist, bei dem durch zumindest einen Verarbeitungsfehler und/oder Zugriffsfehler in einer Ablaufebene zumindest eine Fehlerreaktionsfunktion in zumindest einer der weiteren Ablaufebenen ausgelöst wird.

Dadurch, dass für eine Fehlerreaktionsfunktion eine weitere Ablaufebene, welche eine unterschiedliche Priorität zur ursprünglichen Ablaufebene hat, genutzt wird, ist es möglich die zeitliche Abfolge von Programmen bzw. Funktionen zu beeinflussen. Vorteilhafterweise ist die Wahl der Ablaufebene für die Fehlerreaktionsfunktion programmierbar bzw. parametrierbar.

In einer vorteilhaften Ausgestaltung des Verfahrens zur Fehlerbehandlung wird die Fehlerreaktionsfunktion jeweils in der weiteren Ablaufebene behandelt, welche niederpriorer zu der jeweiligen Ablaufebene ist, in welcher der Verarbeitungs-

fehler und/oder der Zugriffsfehler aufgetreten ist. Dies hat den Vorteil, dass durch den Fehler der zeitliche Ablauf dessen, in welchem der Fehler aufgetreten ist im wesentlichen unbeeinflusst bleibt. Unter Umständen kann jedoch beispielsweise ein einfacher zeitunkritischer Befehl wie die Übernahme eines zuletzt zulässigen Wertes, bei Auftreten eines unzulässigen Wertes durchgeführt werden.

Durch den Verarbeitungsfehler und/oder den Zugriffsfehler ist auch eine Fehlerreaktionsfunktion in derselben Ablaufebene wie der Verarbeitungsfehler und/oder Zugriffsfehler auslösbar, bzw. wird dort ausgelöst, wobei eine weitere Fehlerreaktionsfunktion in zumindest einer niederprioreren Ablaufebene ausgelöst wird.

So ist zunächst eine sichere Weiterbearbeitung des Programmes bzw. der Funktion in welcher der Fehler aufgetreten ist gewährleistet ohne, dass beispielsweise bezüglich der Einhaltung von Echtzeiterfordernissen Probleme entstehen. Eine nicht mehr so zeitkritische Fehlerbehandlung erfolgt dann durch die in einer niederprioreren Ablaufebene gestarteten Fehlerreaktionsfunktion.

Besonders vorteilhaft ist die Durchführung eines Verfahrens zur Fehlerbehandlung bei einem Automatisierungssystem, d.h. bei einer Automatisierungssteuerung, welche als Echtzeit-Automatisierungssystem eingesetzt wird.

Das erfindungsgemäße Verfahren zur Fehlerbehandlung wird also vorteihaft bei Echtzeit-Anforderungen angewandt und erfüllt diese auch. Dies gilt insbesondere für ein Automatisierungssystem mit hochprioren zyklischen Tasks, wobei die Regelungsgüte gewährleistet bleibt. Hohe Anforderungen an Regelgüte und Dynamik eines Automatisierungssystems bleiben gewahrt.

In einer vorteilhaften Ausgestaltung wird die Fehlerreaktionsfunktion vor dem Auslösen dieser, parametriert und/oder programmiert.

Eine Anforderung nach einer flexiblen, sicheren und/oder konsistenten Reaktion auf Fehler ist durch einen durchgängigen konsistenten Gesamtansatz zur Fehlerbehandlung mittels der Definition / Realisierung von:

- Zugriffsfunktionen und/oder
- eines definierten konfigurierbaren Ablaufverhaltens bei Zugriffsfehler bei Nichtanwendung der Zugriffsfunktion und/oder
- eines definierten Verhaltens bei Auftreten von Verarbeitungsfehlern in einem Anwenderprogramm

erfindungsgemäß ermöglicht.

Bei der Definition bzw. Realisierung von Zugriffsfunktionen sind Zugriffsfehler über parametrierbare Zugriffsfunktionen abfangbar, wobei in vorteilhafter Weise die Möglichkeit besteht, bei einem Fehler ein vordefiniertes Verhalten zu erzeugen. Beispiele hierfür sind die Übernahme eines projektierten Ersatzwert, die Übernahme des letzten Wertes und/oder auch das Einsetzen eines Grenzwertes. Das Verhalten der Zugriffsfunktion über Parameter ist vor deren Aufruf bzw. auch unmittelbar beim Aufruf einstellbar. Die Festlegung eines vordefinierten Verhaltens bei einem Fehler einer Zugriffsfunktion ist eine Fehlerreaktionsfunktion. Die Ausführung der Zugriffsfunktion bedingt bei einem Zugriffsfehler nicht zwangsläufig den Start eines Fehlerbearbeitungs-Task, d.h. einer Fehlerreaktionsfunktion welche synonym ist, jedoch ist eine Fehlerreaktionsfunktion ausführbar. Die Zugriffsfunktion ist vorteilhaft in verschiedenen, vorzugsweise jedem, Tasktyp verwendbar.

Beim Auftreten eines Fehlers beispielsweise bei einem Zugriff auf einen internen bzw. externen Wert und einer Nichtanwendung der Zugriffsfunktion ist vorteilhaft ein definiertes konfigurierbares Ablaufverhalten bei zumindest einem Zugriffsfehler realisierbar. Wenn ein Zugriffsfehler auftritt, ohne dass eine Zugriffsfunktion verwendet wird, wird vom Automatisierungssystem bzw. der Automatisierungssteuerung ein konfiguriertes Verhalten wie z.B. die Übernahme des Ersatzwertes, die Übernahme des letzten Wertes, oder der Start einer Fehlerbearbeitungs-Task, in der die Reaktion flexibel ausprogrammiert werden kann, ausgeführt.

Tritt in einem Anwenderprogramm ein Verarbeitungsfehler auf so ist ein definiertes einstellbares Verhalten bezüglich des Verarbeitungsfehlers erfindungsgemäß ermöglicht. Hierfür ergeben sich beispielsweise die folgenden Möglichkeiten:

- Start der Fehlerbearbeitungs-Task, d.h. der Fehlerreaktionsfunktion, bei einem Verarbeitungsfehler im Anwenderprogramm;
- oder direktes Überführen des Automatisierungssystems in den Stop-Zustand.

Die Fehlerbearbeitungs-Task, d.h. die Fehlerreaktionsfunktion weist dabei beispielsweise eine der folgenden Eigenschaften auf:

- in der Fehlerbearbeitungs-Task/Fehlerreaktionsfunktion kann ein Anwenderprogramm zur Reaktion auf den Verarbeitungsfehler oder Zugriffsfehler eingehängt werden;
- der Fehlerbearbeitungs-Task/Fehlerreaktionsfunktion wird in einer Task-Startinformation mitgegeben, in welcher Task der Fehler aufgetreten ist und von welcher Art der Zugriffsfehler oder der Bearbeitungsfehler ist;
- die Fehlerbearbeitungs-Task/Fehlerreaktionsfunktion weist im Ablaufsystem eine definierte Priorität auf, wobei diese im Automatisierungssystem hochpriore zyklische

Tasks, z.B. von Motion Control (Bewegungssteuerung), nicht behindert; die Priorität der Fehlerbearbeitungs-Task ist dabei wahlweise fest oder auch einstellbar, jedoch unterhalb der Prioritätsstufe der hochprioren zyklischen Tasks für z.B. eine Bewegungssteueuerung und/oder eine andere Regelung;

- der Start der Fehlerbearbeitungs-Task/Fehlerreaktionsfunktion führt zu Stop und Abbruch der Task, in deren Anwenderprogramm der Fehler aufgetreten ist;
- nicht-zyklische Tasks können über eine Programmierung in dem Fehlerbearbeitungs-Task/Fehlerreaktionsfunktion neu gestartet werden.

Damit ist ein konsistentes System- und Ablaufverhalten auch in harten Echtzeitsystemen erreichbar.

Durch die erfindungsgemäße Ausgestaltung eines Automatisierungssystems sind Zugriffsfehler direkt in flexible parametrierbare Zugriffsfunktionen abfangbar. Reaktionen auf Zugriffsfehler und Verarbeitungsfehler sind auch in einer Fehlerreaktionsfunktion programmierbar, wobei die Fehlerreaktionsfunktion im Fehlerfall gestartet wird. Die erfindungsgemäße Fehlerbehandlung ist vorteilhafterweise verbunden mit dem Nichtabbruch oder der Nichtbeeinflussung hochpriorer zyklischer Systemtasks, wie diese z.B. bei Motion Control-Aufgaben auftreten. Derartige Aufgaben sind beispielsweise eine Interpolation und/oder eine Regelung.

Mit Hilfe der erfindungsgemäßen Fehlerbehandlung ist ein sicheres Systemverhalten des Automatisierungssystem auch dadurch erreichbar, dass der Task beendbar ist, in welchem ein Fehler aufgetreten ist. In vorteilhafter Weise sind nichtzyklische Tasks neu aufsetzbar, d.h. startbar. Beim Neuaufsetzen nicht-zyklischer Tasks werden entweder die Startwerte des ursprünglichen Tasks verwendet oder aber Zwischenergebnisse des abgebrochenen Tasks.

Die erfindungsgemäße Fehlerbehandlung ist vorteilhafterweise verbunden mit dem Absteuern, d.h. Herunterfahren bzw. Stoppen des Systems bei Auftreten zumindest eines Fehlers in einem zyklischen Task, da in diesem Fall die wiederholte Abarbeitung und/oder der Abbruch des zyklischen Tasks nicht unbedingt sinnvoll ist. In vorteilhafter Weise wird erfindungsgemäß ein konsistentes Systemverhalten erreicht, auch dann, wenn das System nicht in Stop geht.

In einer vorteilhaften Weise wird erfindungsgemäß die maximal zulässige Gesamtlaufzeit eines hochprioren zyklischen Tasks nicht überschritten um eine vereinbarte Regelungs- und/oder Steuerungsgüte zu gewährleisten. Dies gilt insbesondere bei Automatisierungssteuerungen und/oder Automatisierungssystemen, wobei diese Begriffe gleichbedeutend benutzbar sind, mit harten Echtzeitanforderungen.

Das erfindungsgemäße Automatisierungssystem ist vorteilhaft bei einer Produktionsmaschine und/oder einer Werkzeugmaschine eingesetzt.

Weitere vorteilhafte Ausführungen bzw. eine Verwendung und/oder Vorrichtung zur Erfindung sind den Ansprüchen 1 bis 15 entnehmbar.

Ausführungsbeispiele zur Erfindung sind in den Figuren dargestellt. Dabei zeigen

Figur 1 unterschiedliche ablaufebenen zur Ausführung von Software in einem Automatisierungssystem und
Figur 2 Fehlerreaktionsfunktionen verteilt in Ablaufebenen.

Die Darstellung gemäß FIG 1 zeigt fünf verschieden Ablaufebenen 1A, 2A, 3A, 4A und 5A zur Ausführung von Software eines Automatisierungssystems. Eine Priorität P - in der Figur 1 als Pfeil dargestellt, ist von der Ablaufebene 5A bis zur Ablaufebene 1A ansteigend. Abzuarbeitende Tasks T sind in den

Ablaufebenen 1A bis 5A als Balken dargestellt und bezüglich einer Zeitachse Z aufgetragen. Hoch priore Funktionen d.h. Tasks wie z.B. Kommunikationstasks KT werden in der Ablaufebene 1A ausgeführt. Die Kommunikationstasks KT wiederholen sich zyklisch in einem Taktzyklus TZK für die Kommunikation. In einem weiteren Taktzyklus TZI erfolgt die Abarbeitung z.B. für eine Interpolation z.B. einer Werkzeugmaschine oder einer Produktionsmaschine. Die Funktion für die Interpolation wird im Interpolations-Task ausgeführt, wobei die Ausführung in einer zur Ablaufebene 1A niederen Priorität in der Ablaufebene 2A erfolgt. Der Ablaufebene 3A sind Interrupt-Tasks IT zugewiesen. Anwendertasks AT1 und AT2 sind entsprechend ihrer Wichtigkeit den Ablaufebenen 4A und 5A zugeordnet.

Die Darstellung gemäß Figur 2 zeigt beispielhaft verschiedene Tasks NZT, NNT, IT, HZT, HZST und FT, welche in einem Automatisierungssystem ablauffähig sind. Der Begriff Task ist dabei z.B. im Sinne des Begriffs Funktion anwendbar, wobei die Funktion zumindest eine Aufgabe beinhaltet. Eine Funktion ist jedoch auch in verschiede Tasks unterteilbar. In der FIG 2 sind die folgenden Tasks aufgeführt, wobei diese unterschiedliche Prioritäten aufweisen:

- niederpriorer zyklischer Task NZT
- nichtzyklische Tasks NNT
- Fehlerbearbeitungs-Task FT1, FT2, FT3
- Interrupt Tasks IT
- Hochpriore zyklische Tasks HZT
- Hochpriore zyklische System Tasks HZST.

Der Fehlerbearbeitungs-Task entspricht einer Fehlerreaktionsfunktion. Die Tasks NZT, NNT, IT, HZT, HZST und FT sind Ablaufebenen A zugewiesen, wobei die Ablaufebenen A unterschiedliche Prioritäten P bezüglich der Bearbeitung aufweisen und in die Ablaufebenen 1A, 2A, 3A und 4A unterteilt sind. Die Priorität P, welche als nach unten weisender Pfeil dargestellt ist, nimmt in Pfeilrichtung zu. Die Tasks werden durch

rechteckige Kästchen repräsentiert, wobei jedem Kästchen zumindest eine Task zugeordnet ist. Die zeitliche Aufeinanderfolge der Tasks NZT, NNT, IT, HZT, HZST und FT1/2/3 erfolgt durch die perspektivische Darstellung in Bezug auf eine als Pfeil dargestellte Zeitachse Z.

Die Fehlerbearbeitungstasks FT1, FT2, FT3 sind der Priorität nach, verschiedenen Ablaufebenen 1A und 2A zugeordnet. In den entsprechenden Ablaufebenen A finden sich auch die Interrupt Tasks IT und/oder die niederprioren zyklischen Tasks NZT und/oder die niederprioren nichtzyklischen Tasks NNT nebengestellt.

Bei den folgenden Tasks: niederpriorer zyklischer Task NZT niederpriorer nichtzyklischer Task NNT, interrupt Task IT, hochpriorer zyklischer Task HZT und dem Fehlerbearbeitungstask können Zugriffsfunktionen in allen Anwendertasks verwendet werden.

Tritt beispielsweise ein Fehler F in der Ablaufebene 2A des Interrupt Tasks IT auf, so ist eine Fehlerbearbeitungstask FT1 in derselben Ablaufebene 2A startbar. Durch den Fehler kann jedoch auch eine Fehlerbearbeitungstask FT2 bzw. FT3 in einer niederpriorenren Ablaufebene 1A gestartet werden. Das Starten einer niederprioreren Fehlerbearbeitungtask FT2, FT3 kann auch durch eine andere Fehlerbearbeitungstask FT1 erfolgen. Die Ausführung von Fehlerbearbeitungstasks FT1, FT2, d.h. von Fehlerreaktionsfunktionen in einer niederprioreren Ablaufebene spart Rechenzeit eines Rechners für höherpriore Tasks. Damit ist ein Echtzeit-Automatisierungssystem realisierbar. Dieses genügt auch harten Echtzeitanforderungen insbesondere im Fehlerfall.

Patentansprüche

1. Verfahren zur Fehlerbehandlung bei einem Echtzeit-Automatisierungssystem bei dem durch zumindest einen Verarbeitungsfehler (F) und/oder Zugriffsfehler (F) zumindest eine Fehlerreaktionsfunktionsfunktion (FT1, FT2, FT3) ausgelöst wird, wobei die Fehlerreaktionsfunktion (FT1, FT2, FT3) parametrierbar und/oder programmierbar ist.

2. Verfahren zur Fehlerbehandlung bei einem Automatisierungssystem, welches zumindest zwei Ablaufebenen (a, 1A, 2A, 3A, 4A, 5A) aufweist, bei dem durch zumindest einen Verarbeitungsfehler (F) und/oder Zugriffsfehler (F) in einer Ablaufebene (A) zumindest eine Fehlerreaktionsfunktion (FT1, FT2, FT3) in zumindest einer der weiteren Ablaufebenen (A) ausgelöst wird.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Fehlerreaktionsfunktion (FT1, FT2, FT3) jeweils in der weiteren Ablaufebene (A) behandelt wird, welche niederpriorer zu der jeweiligen Ablaufebene (A) ist, in welcher der Verarbeitungsfehler (F) und/oder der Zugriffsfehler (F) aufgetreten ist.

4. Verfahren nach Anspruch 2 oder 3, dadurch gekennzeichnet, dass durch den Verarbeitungsfehler (F) und/oder den Zugriffsfehler (F) eine Fehlerreaktionsfunktion (FT1, FT2, FT3) in derselben Ablaufebene (A) wie der Verarbeitungsfehler (F) und/oder Zugriffsfehler (F) ausgelöst wird und dass eine weitere Fehlerreaktionsfunktion (FT1, FT2, FT3) in zumindest einer niederprioreren Ablaufebene (A) ausgelöst wird.

5. Verfahren nach einem der Ansprüche 2 bis 4, dadurch gekennzeichnet, dass als Automatisierungssystem ein Echtzeit-Automatisierungssystem verwendet wird.

6. Verfahren nach Anspruch 2 oder 5, dadurch gekennzeichnet, dass die Fehlerreaktionsfunktion (FT1, FT2, FT3) vor dem Auslösen parametriert und/oder programmiert wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass Zugriffsfehler (F) mit Hilfe von parametrierbaren Zugriffsfunktionen (FT1, FT2, FT3) abgefangen werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass zumindest hochpriore zyklische Systemfunktionen (HZST) durch die Fehlerreaktionsfunktion (FT1, FT2, FT3) unbeeinflusst ausgeführt werden.

9. Verfahren nach einem der vorgenannten Ansprüche 1 bis 8, dadurch gekennzeichnet, dass zumindest hochpriore zyklische Systemfunktionen (HZST) auch bei Ausführung einer Fehlerreaktionsfunktion (FT1, FT2, FT3) abbruchslos weitergeführt werden.

10. Verfahren nach einem der vorgenannten Ansprüche 1 bis 9, dadurch gekennzeichnet, dass Funktionen, welche eine Fehlfunktion (F) aufweisen, abgebrochen werden, wodurch ein sicheres Verhalten des Automatisierungssystems gewährleistet ist.

11. Verfahren nach einem der vorgenannten Ansprüche 1 bis 10, dadurch gekennzeichnet, dass abgebrochene nichtzyklische Funktionen (NNT) neu gestartet werden, wobei dabei auf die jeweils vorangegangene abgebrochene Funktion (NNT) aufgesetzt wird.

12. Verfahren nach einem der vorgenannten Ansprüche 1 bis 10, dadurch gekennzeichnet, dass bei Fehlern (F) in zyklischen Funktionen (NZT, HZT) das Automatisierungssystem gestoppt wird.

13. Verfahren nach einem der vorgenannten Ansprüche 1 bis 11, dadurch gekennzeichnet, dass beim Auftreten von Fehlern (F) durch das Automatisierungssystem ein konsistentes Systemverhalten erzeugt wird ohne das Automatisierungssystem zu stoppen.

14. Verwendung des Verfahrens nach einem der vorgenannten Ansprüche, dadurch gekennzeichnet, dass die Verwendung bei einer Werkzeugmaschine und/oder einer Produktionsmaschine erfolgt.

15. Vorrichtung zur Durchführung des Verfahrens nach einem der vorgenannten Ansprüche, dadurch gekennzeichnet, dass die Vorrichtung ein Automatisierungssystem ist.

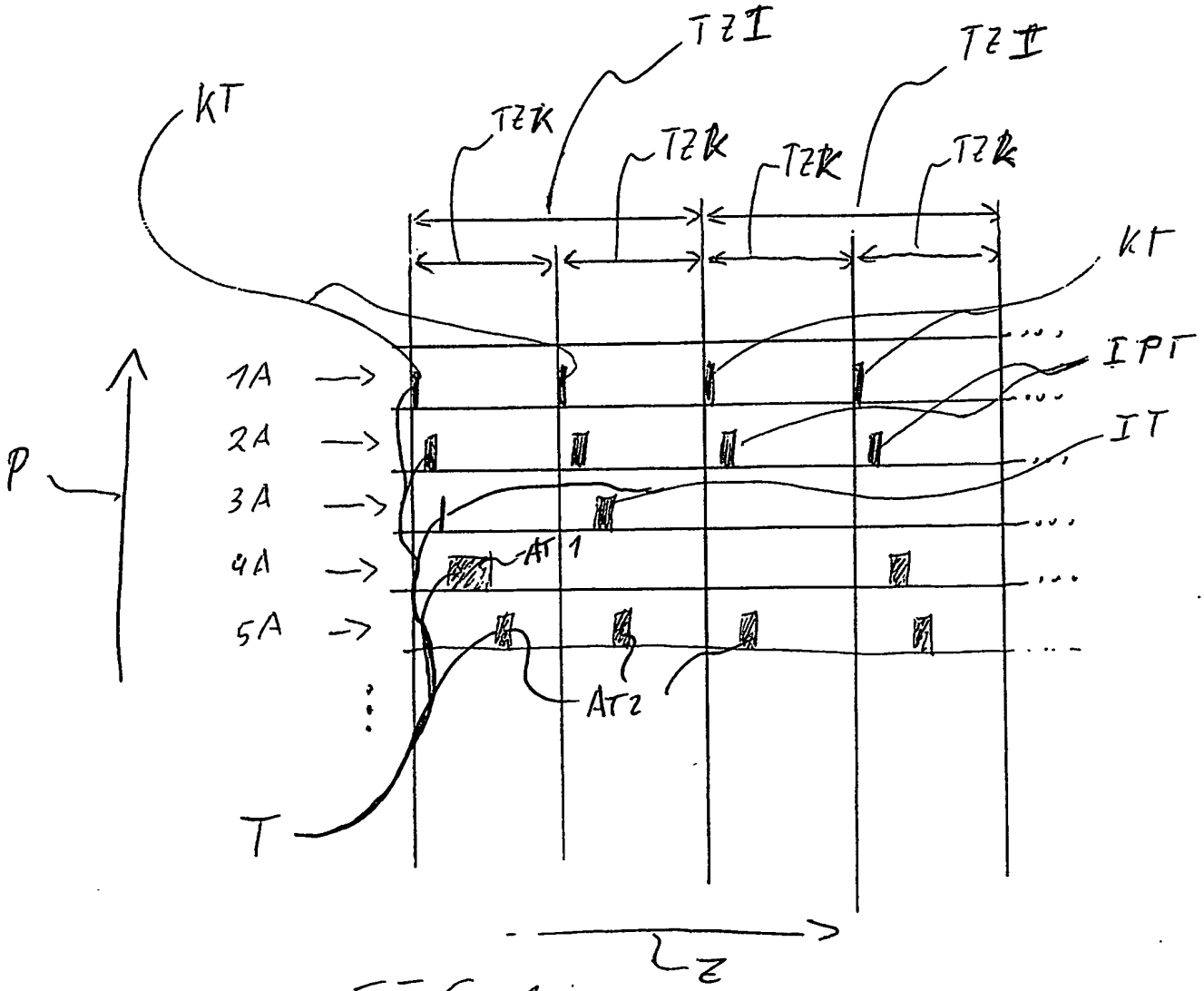


FIG 1

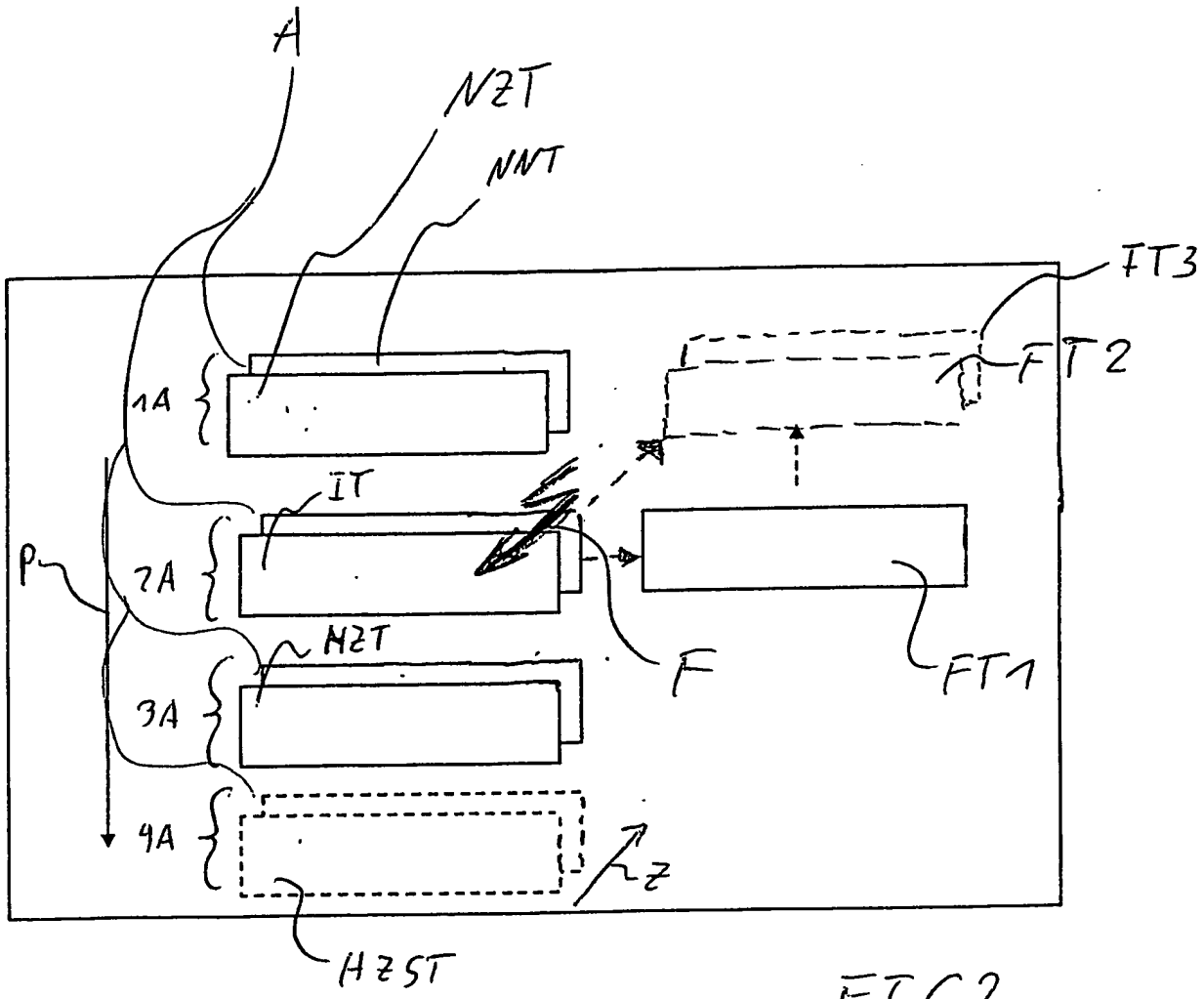


FIG 2

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
10. Juli 2003 (10.07.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2003/056428 A3

(51) Internationale Patentklassifikation[7]: G06F 11/00, G05B 19/042, G06F 11/07

(21) Internationales Aktenzeichen: PCT/DE2002/004711

(22) Internationales Anmeldedatum:
23. Dezember 2002 (23.12.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 64 495.7 28. Dezember 2001 (28.12.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KRAM, Raimund** [DE/DE]; Fliederstr. 7a, 91056 Erlangen (DE). **BIRZER, Johannes** [DE/DE]; Friedhofweg 2, 92551 Stulln (DE). **HORN, Wolfgang** [DE/DE]; Maria-Reiff-Weg 5, 09337 Hohenstein-Ernstthal (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

(81) Bestimmungsstaat *(national)*: US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

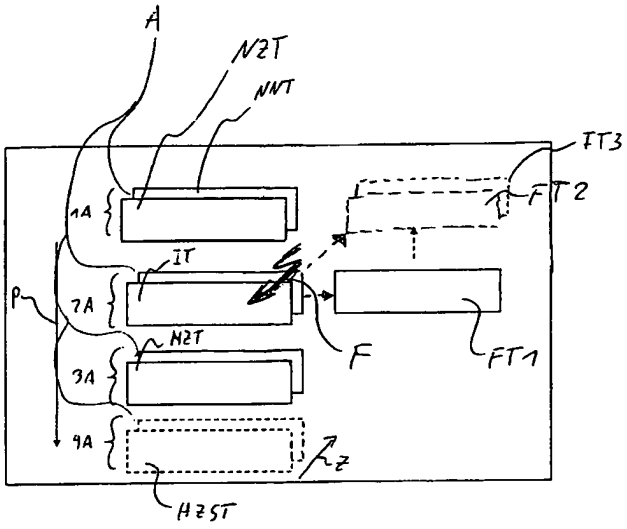
Erklärungen gemäß Regel 4.17:

— *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR)*

[Fortsetzung auf der nächsten Seite]

(54) **Title:** ERROR TOLERANT AUTOMATION SYSTEM OR METHOD FOR ERROR TREATMENT IN A REAL TIME AUTOMATION SYSTEM

(54) **Bezeichnung:** FEHLERTOLERANTES AUTOMATISIERUNGSSYSTEM BZW. VERFAHREN ZUR FEHLERBEHANDLUNG BEI EINEM ECHTZEIT-AUTOMATISIERUNGSSYSTEM



(57) **Abstract:** The invention relates to an automation system, wherein error (F) reaction is improved. This is achieved by means of a method for the treatment of errors in a real time automation system wherein at least one error reaction function (FT1, FT2, FT3) is triggered by at least one processing error (F) and/or access error (F). Said improvement is achieved by means of a method for the treatment of errors wherein the error reaction function (FT1, FT2, FT3) and by means of a method for the treatment of errors in an automation system which has at least two levels of execution (A), wherein at least one error reaction function (FT1, FT2, FT3) is triggered by at least one processing error (F) and/or one access error (F) on at least one of the other levels of execution (A).

[Fortsetzung auf der nächsten Seite]

WO 2003/056428 A3

— *Erfindererklärung (Regel 4.17 Ziffer iv) nur für US*

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 5. Februar 2004

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Automatisierungssystem, bei welchem die Reaktion auf Fehler (F) verbessert ist. Dies gelingt zum einen mit einem Verfahren zur Fehlerbehandlung bei einem Echtzeit-Automatisierungssystem bei dem durch zumindest einen Verarbeitungsfehler (F) und/oder Zugriffsfehler (F) zumindest eine Fehlerreaktionsfunktionsfunktion (FT1, FT2, FT3) ausgelöst wird, wobei die Fehlerreaktionsfunktion (FT1, FT2, FT3) parametrierbar und/oder programmierbar ist. Zum anderen gelingt eine Verbesserung durch ein Verfahren zur Fehlerbehandlung bei einem Automatisierungssystem, welches zumindest zwei Ablaufebenen (A) aufweist, bei dem durch zumindest einen Verarbeitungsfehler (F) und/oder Zugriffsfehler (F) in einer Ablaufebene (A) zumindest eine Fehlerreaktionsfunktion (FT1, FT2, FT3) in zumindest einer der weiteren Ablaufebenen (A) ausgelöst wird.

INTERNATIONAL SEARCH REPORT

Internatio pplication No
PCT/DE [redacted]4711

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/00 G05B19/042 G06F11/07

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
INSPEC, EPO-Internal, COMPENDEX, PAJ, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	STEWART D B ET AL: "The Chimera II real-time operating system for advanced sensor-based control applications" IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS, NOV.-DEC. 1992, USA, vol. 22, no. 6, pages 1282-1295, XP000355586 ISSN: 0018-9472	1-3,5-7, 10-15
Y	page 1282, left-hand column, line 25 - line 29 page 1284, right-hand column, paragraph 3 -page 1285, left-hand column, paragraph 1 page 1287, right-hand column, line 3 -page 1288, left-hand column, line 42	4,8,9

-/--

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 December 2003	16/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lanchès, P

INTERNATIONAL SEARCH REPORT

Internatic Application No
PCT/DE [redacted]4711

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	STEWART D B ET AL: "Dynamically reconfigurable embedded software-does it make sense?" ENGINEERING OF COMPLEX COMPUTER SYSTEMS, 1996. PROCEEDINGS., SECOND IEEE INTERNATIONAL CONFERENCE ON MONTREAL, QUE., CANADA 21-25 OCT. 1996, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 21 October 1996 (1996-10-21), pages 217-220, XP010201560 ISBN: 0-8186-7614-0 page 220, left-hand column, line 9 - line 43	4,8,9
A	TERRASA A ; GARCIA-FORNES A ; BOTTI V : "Including user-defined timing exception support in FRTL " PROCEEDINGS SEVENTH INTERNATIONAL CONFERENCE ON REAL-TIME COMPUTING SYSTEMS AND APPLICATIONS , 12 - 14 December 2000, pages 255-262, XP009022132 Los Alamitos, CA, USA page 255, right-hand column, line 22 -page 257, left-hand column, line 5 page 258, right-hand column, line 2 - line 37 page 260, left-hand column, line 3 - line 35	1-15

INTERNATIONALER RECHERCHENBERICHT

Internatio Aktenzeichen
PCT/DE [redacted]4711

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F11/00 G05B19/042 G06F11/07

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
INSPEC, EPO-Internal, COMPENDEX, PAJ, IBM-TDB, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	STEWART D B ET AL: "The Chimera II real-time operating system for advanced sensor-based control applications" IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS, NOV.-DEC. 1992, USA, Bd. 22, Nr. 6, Seiten 1282-1295, XP000355586 ISSN: 0018-9472	1-3,5-7, 10-15
Y	Seite 1282, linke Spalte, Zeile 25 - Zeile 29 Seite 1284, rechte Spalte, Absatz 3 -Seite 1285, linke Spalte, Absatz 1 Seite 1287, rechte Spalte, Zeile 3 -Seite 1288, linke Spalte, Zeile 42	4,8,9

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[ ] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
'A' Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
'E' älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
'L' Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
'O' Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
'P' Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
'T' Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
'X' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
'Y' Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
'&' Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
3. Dezember 2003	16/12/2003

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lanchès, P

INTERNATIONALER RECHERCHENBERICHT

Internatio Aktenzeichen
PCT/DE [redacted]04711

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	STEWART D B ET AL: "Dynamically reconfigurable embedded software-does it make sense?" ENGINEERING OF COMPLEX COMPUTER SYSTEMS, 1996. PROCEEDINGS., SECOND IEEE INTERNATIONAL CONFERENCE ON MONTREAL, QUE., CANADA 21-25 OCT. 1996, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 21. Oktober 1996 (1996-10-21), Seiten 217-220, XP010201560 ISBN: 0-8186-7614-0 Seite 220, linke Spalte, Zeile 9 - Zeile 43 ---	4,8,9
A	TERRASA A ; GARCIA-FORNES A ; BOTTI V : "Including user-defined timing exception support in FRTL " PROCEEDINGS SEVENTH INTERNATIONAL CONFERENCE ON REAL-TIME COMPUTING SYSTEMS AND APPLICATIONS , 12. - 14. Dezember 2000, Seiten 255-262, XP009022132 Los Alamitos, CA, USA Seite 255, rechte Spalte, Zeile 22 -Seite 257, linke Spalte, Zeile 5 Seite 258, rechte Spalte, Zeile 2 - Zeile 37 Seite 260, linke Spalte, Zeile 3 - Zeile 35 -----	1-15